Task 5

So far, we have defined security against a passive adversary that only eavesdrops and an active adversary that can carry out a chosen plaintext attack. A chosen cipher attack is even more powerful. In cca, adversary has the ability to encrypt any plaintext as in cpa as well as decrypt any ciphertext of its choice.

CCA indistinguishability experiment says:

1) An adversary A is given input 1 ^n and oracle access to Enck() and Deck(). It outputs a pair of messages m0, m1 of the same length.
2) A random bit b <- {0,1} is chosen and then a ciphertext c <- Enck(m0) is computed and given to A. We call c as the challenge ciphertext.
3) The adversary continues to have the oracle access, except Deck() on the challenge ciphertext c itself.
4) The output of the experiment is defined to be 1 if b' = b, and 0 otherwise.

Hence, a private key encryption scheme has indistinguishable encryptions under CCA if for all probabilistic polynomial time adversaries A and negligible function negl,

$$Pr[PrivK^{cca}_{A;\Pi}(n) = 1] \leq 0.5 + negl(n);$$

CCA therefore defines non-malleable encryption scheme, it is such that if the adversary tries to modify the cipher text, the result is either an invalid cipher text or it encrypts the plaintext such that it has no relation to previous one.

Build Algorithm

To achieve CCA security, we construct a scheme such that the adversary will not be able to obtain any valid ciphertext that was not generated by legitimate parties. Thus, we first encrypt our message than calculate a MAC on that encrypted text, this way any change in the ciphertext created by an adversary will not be valid.

Encryption Algorithm: Takes Keys k1 and k2 and message m as input. It encrypts the message using key k1 and calculates tag on this encrypted message.

Receiver on receiving the message from the sender, first calculates the mac on the encrypted text received, checks it with the received mac, if they match, proceeds to decrypt and consume the message otherwise rejects it.

Proof

Theorem: Assume that *that* $\Pi_E = (Gen_E, Enc, Dec)$ is a CPA secure encryption scheme and that $\Pi_M = (Gen_M, Mac, Vrfy)$ is a secure message authentication code with unique tags, then the above stated algorithm is CCA secure.

The idea behind the proof is, since we have a secure mac, we can assume that all queries to decryption oracle are invalid, unless the cipher text itself was previously obtained by the adversary. Therefore, we can assume that the CCA security is reduced to security of CPA scheme itself. Therefore, we can first prove that the only valid queries to the oracle are ciphertexts that were previously obtained excepting negligible probability otherwise. Then, we can prove that if

CCA is not secure, CPA must also not be secure which will be a contradiction, since, we have already proven CPA security.

Let A be any probabilistic polynomial-time CCA adversary attacking our algorithm. We defined a valid query, valid-queryA;Π'(n) to be the event that such that A generates a query(c, t) to the decryption oracle that was not obtained from the encryption oracle. We say that, Pr[valid-queryA;Π'(n)] is at most negligible. Thus, if (c, t) was not obtained by querying the encryption oracle, this means that A must have forged the MAC. Therefore, we can say that for some negligible function negl,

$$\Pr[\text{valid-query}_{A;\Pi'}(n)] < \text{negl}(n):$$

Given that, valid-query occurs with at most negl() probability, we now reduce the cca security to cpa security. Let A be a probabilistic polynomial time adversary for $\text{PrivK}_{\text{cca}}$. We construct adversary A_{enc} for the CPA experiment with (Gen_E; Enc; Dec). Adversary A chooses a key k2 and invokes the adversary. Whenever, A asks encryption query q, A queries its encryption oracle with q and receives back some cipher, c. Then it computes its mac and finally has (c, t). When A asks A_{enc} the decryption of the same, it checks if (c, t) was generated in a previous query, if yes, than hands A the original q or if no, then hands a null response to A. When A outputs a pair (q0, q1) representing two queries. adversary A_{enc} outputs the same pair and receives back a challenge ciphertext c. A_{enc} hands A the challenge cipher text (c, t) where t = MACk2(c). Now, A_{enc} does not need decryption oracle as it assumes any new query is always invalid. Therefore, the success of A_{enc} in PrivKcpa when a valid query does not occur equals the success of A in PrivKcca when valid query does not occur.

$$\begin{aligned}\Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A}_{\text{enc}},\Pi_E}(n) = 1 \wedge \neg\text{VALID-QUERY}_{\mathcal{A},\Pi'}(n)] \\ = \Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi'}(n) = 1 \wedge \neg\text{VALID-QUERY}_{\mathcal{A},\Pi'}(n)]]\end{aligned}$$

implying that

$$\begin{aligned}&\Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A}_{\text{enc}},\Pi_E}(n) = 1] \\ &\quad \geq \Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A}_{\text{enc}},\Pi_E}(n) = 1 \wedge \neg\text{VALID-QUERY}_{\mathcal{A},\Pi'}(n)] \\ &\quad = \Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi'}(n) = 1 \wedge \neg\text{VALID-QUERY}_{\mathcal{A},\Pi'}(n)]\end{aligned}$$

Assume now by contradiction that there exists a *non-negligible function* ε such that

$$\Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi'}(n) = 1] = \frac{1}{2} + \varepsilon(n).$$

By the fact that $\Pr[\text{VALID-QUERY}_{\mathcal{A},\Pi'}(n)]$ is negligible, we have that it is smaller than $\varepsilon(n)/2$. This in turn implies that

$$\Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi'}(n) = 1 \wedge \text{VALID-QUERY}_{\mathcal{A},\Pi'}(n)] < \varepsilon(n)/2$$

and so

$$\begin{aligned}\Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi'}(n) = 1] &= \Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi'}(n) = 1 \wedge \neg\text{VALID-QUERY}_{\mathcal{A},\Pi'}(n)] \\ &\quad + \Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi'}(n) = 1 \wedge \text{VALID-QUERY}_{\mathcal{A},\Pi'}(n)] \\ &< \Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi'}(n) = 1 \wedge \neg\text{VALID-QUERY}_{\mathcal{A},\Pi'}(n)] + \frac{\varepsilon(n)}{2}.\end{aligned}$$

Rearranging the above, and using the fact that $\mathcal{A}$ succeeds in $\mathsf{PrivK}^{\mathsf{cca}}$ with probability $1/2 + \varepsilon(n)$, we have that

$$\begin{aligned}\Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi'}(n) = 1 \wedge \neg\text{VALID-QUERY}_{\mathcal{A},\Pi'}(n)] &> \Pr[\mathsf{PrivK}^{\mathsf{cca}}_{\mathcal{A},\Pi'}(n) = 1] - \frac{\varepsilon(n)}{2} \\ &= \frac{1}{2} + \frac{\varepsilon(n)}{2}.\end{aligned}$$

Combining this with Equation (4.5), we have that

$$\Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A}_{\mathrm{enc}},\Pi_E}(n) = 1] > \frac{1}{2} + \frac{\varepsilon(n)}{2}$$